Optimized Video Steganography Using Cuckoo Search Algorithm

Sameh A. Abbas[1]
Dev. Of CS, Dept. of Math.
Faculty of Science, ASU
Cairo, Egypt
Samehamr_83@yahoo.com

Taha I. B. El Arif
Department of Computer Science
Faculty of Computer and Information Science, ASU
Cairo, Egypt
taha_elarif@cis.asu.edu.eg

Fayed F. M. Ghaleb[1]
fayad_ghaleb@sci.asu.edu.eg

Sohier M. Khamis[1]
soheir_khamis@sci.asu.edu.eg

***Abstract*— *Steganography is a process of concealing the secret information into cover object such as text, audio, image, and video. In this paper, we propose a new treatment of Cuckoo Search (CS) algorithm to solve the problem of video steganography. CS is a metaheuristic search algorithm which was recently devolved by Xin-She Yang and Suash Deb in 2009, inspired by the cuckoo bird breeding behavior. The suggested algorithm is based on taking secret data byte by byte. The bits of each byte are arranged to obtain five different forms. The next step focuses on searching about the best carrier pixel in the cover frame. The best pixel is determined using Euclidian distance which evaluate the similarity between the pixels and different byte forms. The random move from pixel to another is achieved using Lévy flight random walk. Finally, the suitable carrier pixel is detected and embedded in its RGB components using the 3-3-2 Least Significant Bit (LSB) replacement technique. In addition, each secret image's color component is embedded separately into a selected cover video's frame. Results show that CS is superior to Genetic Algorithm (GA) and the base technique in term of Peak Signal to Noise Ratio (PSNR).*

Keywords*— *Video Steganography; Cuckoo Search; Lévy flight; LSB; PSNR.

I. INTRODUCTION

Due to the rapid growth in the use of internet, a large number of information has been shared and transferred through it [1]. The importance of reducing a chance of the information being detected during the transmission is being an important topic nowadays. Steganography has become one of the most robust techniques to transmit confidential messages between parties by hiding the message in some file which third party can't recognizes that message which is existed [2]. Video steganography is the process of concealing some secret information within a video [3].

The biggest advantages of video are the large amount of data that can be concealed inside without being observed and the fact that it is a moving stream of image. The Video based steganography is mainly divided into two methods as mentioned in [4] and [5]. One of them is the *frequency domain method*. In this method, frames are transformed to frequency components by using Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), or Discrete Wavelet Transform (DWT). And then messages are concealed in previously obtained transformed coefficients. Concealing may be bit level or in block level. The other method is the *spatial domain*. The bits of the secret message can be concealed in intensity pixels of the video frames in LSB positions, directly. However, most of the LSB Techniques are prone to attacks [4].

Video steganography can be also divided into lossless and lossy steganography. *Lossless* steganography retrieves both hidden message and original video file without any modifications. *Lossy* steganography, in the other hand, retrieves the hidden message correctly while the original video has some errors. However, the lossy steganography requires store the data at some LSB location or at a specific pixel location. This is easy to implement and it can be apply in real time application with any normal system specifications [6].

There are two important factors have a type of contradiction that every successful steganography system should take into consideration, which are embedding efficiency and embedding payload. The former means good quality of stego data and less amount of host (carrier) data are going to be changed. While the latter means the capacity of secret information to be hidden inside host data is large [7].

As mentioned in [8], CS is one of the most recent intelligent algorithms that can be chosen as a comprehensive search method in many optimization problems.

The suggested approach in this paper is a kind of video steganography in spatial domain. This approach is based on trying to get a large data-hiding capacity with minimal distortion in the host video stream. In this approach, CS is

used to find the best pixels locations in cover frames, where the secret message can be concealed. The founded carrier pixels are concealed in its RGB components using the 3-3-2 LSB replacement technique. The entered secret bytes are restructured according to different five pre-indexed patterns before embedding. In addition, these secret bytes are not embedded in the same order. So, it is difficult for attacker to retrieve the secret information from stego-video.

The rest of this paper is organized as follows. Section 2 presents a description of video steganography. In Section 3, some selected related works are investigated. Section 4 introduces the Cuckoo Search algorithm. In Section 5, the suggested video steganography approach is described. The experimental results and concluded remarks are demonstrated in Sections 6 and 7, respectively.

II. VIDEO BASED STEGANOGRAPHY

Steganography is "a process of embedding the secret information inside the host medium (text, audio, image, and video)" [7]. Its ultimate objectives are un-detectability and robustness of the hidden data. Video is simply comprises of stream of frames (images) and audio. Any frame of the video can be selected for concealing the secret data [9]. The big advantage with video based steganography technique is that a long secret message can be concealed behind it.

The quality of video depends upon a set of parameters such as the number of pixels in a frame, the number of frames per second (fps), and frame's size. The parameter fps is often standard (between 24 and 30 fps) in many common video formats, however, the other two parameters are altered from one video standard to another. Each frame consists of pixels having three or four color components such as RGB (Red–Green–Blue) or CMYK (Cyan–Magenta–Yellow–Black) [10].

The basic model of video based steganography can be illustrated in four basic elements as shown in Fig. 1.

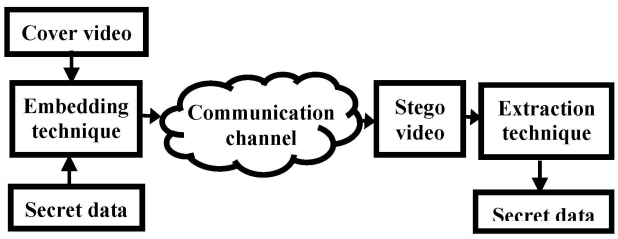

Fig.1. Generalized block diagram of video steganography procedure.

These basic elements are given in the following:

- Cover video: the input video used for data concealing.
- Secret message: the secret data that is to be hidden.
- Embedding algorithm/technique: the procedure to conceal secret message behind cover Video.
- Stego video: it is the digital video that has the secret message hidden inside.

LSB is a popular algorithm used to embed the information in a cover file [11], [12]. Modifying LSB values is necessary for embedding the secret message inside the cover image (which is the carrier). The secret message is decomposed and concealed into the last r bits of a cover image so that hackers cannot notice it.

In the simple LSB, the secret message size which can be embedded is equal to 12.5% of the cover image's size. Thus, it is considered small storage capacity. Consequently, some researchers later used the base technique [12] concealing the message: 3-3-2. In this method as shown in Fig. 2, the first 3 bits of the message are embedded into the last three bits of the Red component; the second 3 bits into the last 3 bits of the Green component; and the last 2 bits in the last 2 bits of the Blue one. Since the variation in blue is perceptible more than both red and green to the human eye, the researchers choose to put only 2 bits in the Blue component.

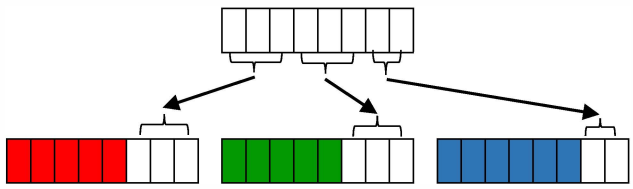

Fig. 2. One Byte of secret information embedded in 3, 3, 2 bit position of LSB of RGB respectively of the cover frame.

This means we have been able to hide byte in each pixel of true color image (24-bit), as shown in Fig. 2. So, it is increased the proportion of concealment by 33.3% from the size of the cover file.

Steganography in video can be divided into two main classes. One is embedding data in uncompressed raw video, which is compressed later [13], [14]. The other tries to embed data directly in compressed video stream [4].

In this paper, we simply consider the steganography in the uncompressed video in spatial domain using the 3-3-2 LSB replacement technique for concealing the confidential message.

III. RELATED WORKS

In recent years, a growing number of video steganography methods and techniques have been developed. These techniques and methods are utilized in various contexts and studied as follows.

In [11], a 3-3-2 LSB based technique is enhanced using Genetic Algorithm (GA) to get an optimal imperceptibility of hidden data. The obtained results have shown that Peak Signal Noise Ratio (PSNR) lies between 20 and 40 decibels (dBs).

A new approach for video steganography has been provided in [12]. The separate frames of the file video are used to hide a size of information equal to around 33.3% of the size of all cover frames using 3-3-2 LSB without visually change.

Another approach that is used to hide a secret video stream in cover video stream, has been proposed in [1]. Utilizing XOR with secret key the 8-bit binary values of secret frames are encrypted and sequentially encoded in cover frames using LSB

in the form of pattern BGRRGBGR. The obtained results have shown that there is no visual distortion in the host video and acceptable quality of recovered secret video.

The Hamming code (7, 4) has been employed for video steganography in [7]. In a multi-phases process, firstly, both cover videos and a secret message are randomly reordered by using a private key. Then, the secret message is concealed using the Hamming code (7, 4). Random values are generated by XOR function and added to the concealed message. Finally, a random area in each frame is selected for the embedding process. The experimental results have shown efficiency of the proposed approach and in general, PSNR is greater than 51 dBs.

A random byte hiding and LSB have been applied for video steganography in [6]. The obtained results have shown that encryption time and decryption time of random byte hiding technique and LSB based steganography are (32.97, 26.3537) and (76.514, 81.04), respectively. Also the hiding ratio (hidden bytes/frame size) for random byte hiding technique and LSB based steganography are 0.002083333 and 0.125, respectively.

IV. CUCKOO SEARCH

Cuckoo Search (CS) is a nature-inspired metaheuristic algorithm developed by Xin-she Yang and Suash Deb in (2009, [8]). It was inspired by the breeding behavior of cuckoos, the cuckoo breeding can be illustrated as an act of parasitism, by laying its egg in a random nests of other host birds (of other species) [15]. Sometimes, these other birds discover the alien egg and throw these alien eggs away or simply abandon nest. A cuckoo might have the characteristic of shape, size, and color of the host eggs to protect it from being discovered. It might take an aggressive action by removing other native eggs from the host nest to increase the hatching probability of their own eggs. A hatched cuckoo chick might even throw other eggs away from the nest to improve its feeding share [15].

CS depends on Lévy flight as the random walk, which is used to produce a new mixture (cuckoos) from current solution according to (1).

$$x_i^{(t+1)} = x_i^{(t)} + \propto \oplus Lévy(s, \lambda) \quad (1)$$

where $x_i^{(t+1)}$ is the i^{th} Cuckoo at instance t+1;

α is the step size; λ is the lévy distribution coefficient.

The lévy flight essentially provides a random walk while the random step length is drawn from a Lévy distribution in (2).

$$Lévy(s, \lambda) \sim s^{-\lambda}, \quad (1 < \lambda \leq 3) \quad (2)$$

The incidental walk via Lévy flight is more efficient in exploring the search space, as its stride length is much longer on the long term.

Cuckoo search has a fewer parameters that need to be tuned when compared with other techniques, in contrast, Particle Swarm Optimization (PSO) needs tuning of mainly three parameters (Inertia weight, effect of self-confidence and effect of social impact), where the range of tuning of PSO's parameters noticeably disturb the attribute of search [16]. In GA, the crossover rate as well the mutation rate needs to be tuned and various selection methodologies need to be selected. In addition, Yang and Deb have discovered that the random-walk style search is better performed by Lévy flights rather than simple random walk [8].

Cuckoo search idealized rules can be summarized as follows [3].

1. Each cuckoo lays one egg at a time, and dumps its egg in a randomly chosen nest.
2. The best nests with high quality of eggs would carry over the next generations.
3. The number of available host nests is fixed and the probability of discovering the laid egg by the host bird can be calculated as $P_a \in [0, 1]$. The fraction pa of the n nests is replaced by new nests (with fresh random solutions).

In [8], a pseudo code of CS is outlined as shown in Fig. 3.

Begin
Objective function: $f(X),\ X = (x_1, x_2, \ldots, x_d)^T$
Generate initial population of
n host nests X_i*= (i =1, 2, ..., n);*
While *(t < MaxGeneration) or (stop criterion)* **DO**
Get a cuckoo randomly by Lévy flights
evaluate its quality/fitness F_i
Choose a nest among n (say, j) randomly
if ($F_i > F_j$),
Replace j by the new solution;
End
A fraction (P_a) *of the worse nests*
are abandoned and new ones are built;
Keep the best solutions/nests;
Rank the solutions and find the current best;
end while
Postprocess results and visualization
end

Fig.3. Pseudo code of the Cuckoo Search (CS).

V. THE SUGGESTED APPROACH

The main idea of the suggested algorithm is to conceal a secret message into a carrier video. This approach depends on selecting suitable RGB pixel values from the cover frames which are chosen by using CS optimization algorithm for concealing the secret message.

At the beginning, a carrier video is converted to frames and audio. Though both audio and frames can be used to embed secret data. A set of frames have been used as the carrier in our suggested approach. The selected carrier frame(s) is given as input to the suggested approach.

As shown in Fig. 4, the suggested approach is comprised of three successive stages: Initialization stage, stage of detecting the best location for embedding and embedding stage.

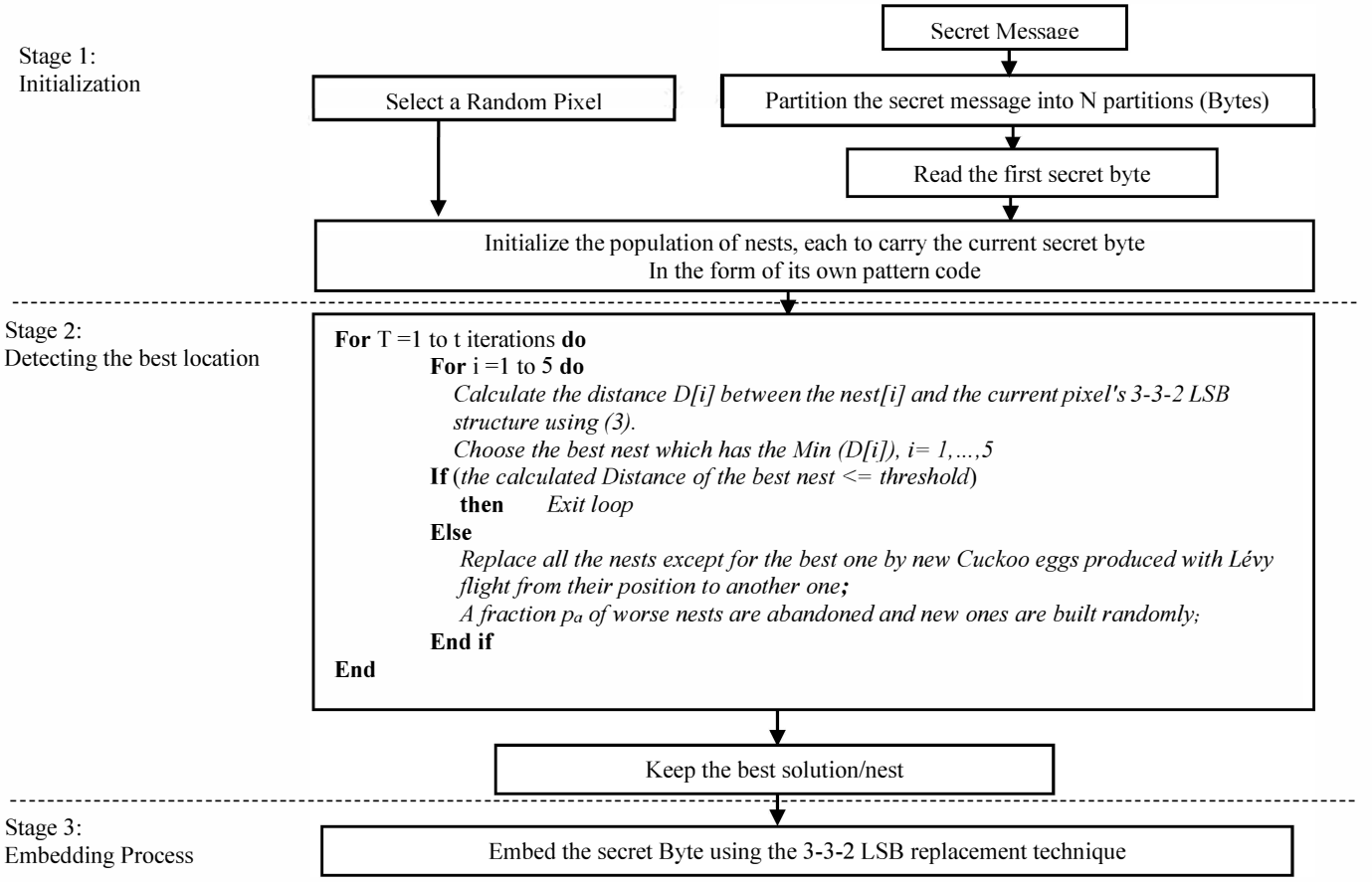

Fig. 4. Suggested video based steganography approach

The aforementioned operation would be consecutively repeated to embed all of the secret bytes. After all of the secret bytes are embedded, the output of the suggested approach is stego frame(s).

Stage One: initialization.

A. Construction of the Different Patterns

During the implementation, the proposed system reads the secret message byte by byte. Each byte is divided into 3-3-2 bit sections noted as R, G, and B, respectively.

Then, these three sections are mutated in different 5 forms to construct the different 5 patterns for the current byte as shown in Fig. 5.

The main aims of these mutations are to increase both, the security level of the information to be hidden and the chance of matching the secret byte with carrier pixel's LSB.

B. Encoding

Fig. 6, shows the typical structure of the nest.

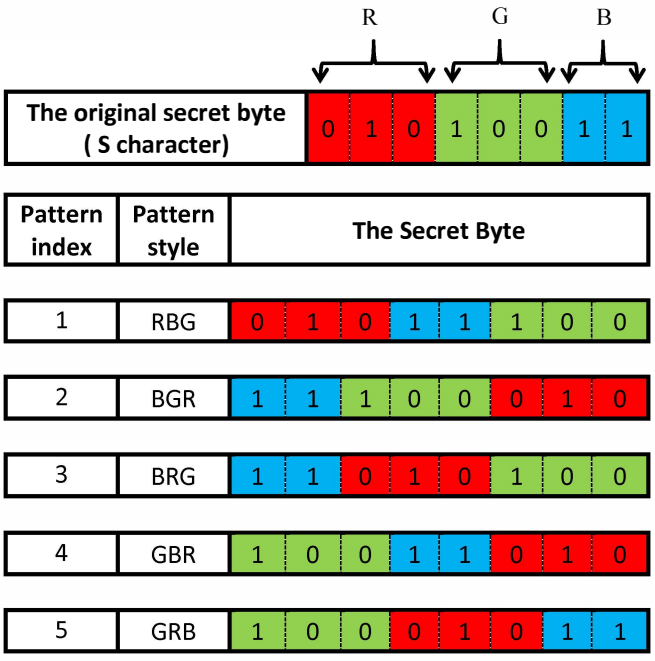

Fig. 5. The different Patterns of the population.

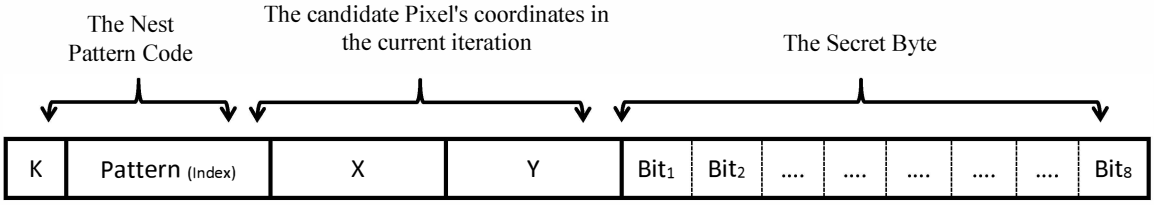

Fig. 6. The Nest Structure.

C. Objective function

The current secret byte will be embedded into the selected pixel's RGB 3-3-2 LSB components. In the proposed approach, the secret byte is divided into 3-3-2 bit sections. Also, the pixel's 3-3-2 LSB sections are extracted. During the search, a cost is calculated for each candidate solution (nest) by calculating the Euclidean distanced between the decimal value of the 3-3-2 LSB sections and the corresponding decimal value of the secret byte sections using the following Euclidean distance equation:

$$D_{SB,\ LSB} = \sqrt{\sum_{Section=1}^{3}(x_{LSB.Section} - x_{SB.Secton})^2}, \quad (3)$$

where *SB* is the current secret byte and *LSB* is the current pixel's 3-3-2 LSB.

For instance, suppose that the current pixel's RGB components and the current secret byte are given as follows.

	Section1	**Section2**	**Section3**
LSB	10001010 (2)	10101010 (2)	10000011 (3)
Secret byte	101 (5)	010 (2)	10 (2)

The objective function will be calculated as follows.

$$D = \sqrt{(2-5)^2 + (2-2)^2 + (3-2)^2}$$

The less cost is the better solution.

D. Setting up Cuckoo Search Algorithm for video steganography

Table I. shows the parameters used for the applied cuckoo search.

TABLE I. TUNING PARAMETERS.

Parameter value	**value**
Number of nests	5
Discovery rate of alien solutions (p_a)	Variant
Lévy exponent (β)	1.5
Maximum Iteration	100
Number of dimensions	2
Lower bounds of search space	Coordinate (1,1)
Upper bounds of search space	Coordinate (frame's height , frame's width)

Stage Two: Detecting the best location using CS.

On applying the Cuckoo search, on each iteration, the following steps should be applied.

A. Updating Nests

All the nests should be updated continuously using Lévy flight as mentioned in (1).

B. Removing of Nests

On the discovery of alien eggs in its nest, a host bird would either get rid of these eggs or quit its nest altogether in quest of setting up a new one elsewhere. Hence, some nests might be removed which is in line with the host bird's attitude.

To simulate this behavior, a fraction P_a of nests representing candidate solution is removed from iteration and new nests are randomly included to substitute them, this action would prevent the search from being stuck at a local optimum point and ensure a better exploration of search space.

C. Elitist selection

Elitist selection indicate that the best solution is kept unaltered and automatically prorogates from iteration to another except if a better solution is found, this concept is still applied in our approach.

Stage Three: Embedding Process.

After founding the best location, i.e. referring to the optimal carrier pixel, we can embed the secret byte in the LSB of RGB (Red, Green and Blue) pixel value of this carrier pixel in 3, 3, 2 order respectively. At first, three bits of the secret byte are concealed inside three bits of LSB of Red pixel, next three bits in the three bits of LSB of Green pixel. Finally, the remaining two bits of secret byte are concealed in two bits of LSB of Blue pixel.

VI. EXPERIMENTAL RESULTS

A. Dataset

To test and evaluate the proposed approach, three cover videos are considered, details of each are given in Table II.

TABLE II. COVER VIDEO FILE DETAILS

S.No.	**Cover Video File information**				**Secret message Resolution (W*H)**
	Name of video	**Resolution (W*H)**	**Frame/sec**	**No. of frames**	
01	Tree.avi	320*240	30	450	150*150
02	globe.avi	320*240	30	107	
03	computer.avi	320*240	30	510	

B. Evaluation Criteria

To evaluate the performance of the suggested approach, MATLAB simulations are performed.

The PSNR [4] given by (4) and Mean square error (MSE) given by (5) are chosen as objective measure to evaluate the proposed scheme.

$$PSNR = 10log_{10}\frac{L^2}{MSE}, \quad (4)$$

where, L is peak signal level for an image color component a ($a \in [r, g, b]$) respectively it is taken as 255. The value of MSE is calculated in (5).

$$MSE = \frac{1}{H \times W}\sum_{i=1}^{H}(I_{i,j} - I'_{i,j})^2, \quad (5)$$

where, $I_{i,j}$ represents original frame and $I'_{i,j}$ represents corresponding stego frame having resolution of $H \times W$ pixels.

C. Results

In the suggested approach, RGB component values are separately extracted. Then, each color component of them is concealed into the selected pixels of a separate carrier frame. Table III shows the performance of the suggested approach.

TABLE III. PERFORMANCE OF SUGGESTED CUCKOO SEARCH OVER VIDEO STEGANOGRAPHY

Name of video	Results obtained using Suggested CS	Results obtained using 3,3,2 LSB	Results obtained using GA as in [11]
	PSNR		
Tree.avi	51.62	38.03	39.37
globe.avi	47.74	32.67	34.37
computer.avi	54.23	39.21	41.61

Generally, when the PSNR value is higher than 30 dBs, the quality of the obtained stego-video is acceptable [17]. As shown in Table III, the proposed method does not cause a significant decrease in video quality. All the results of PSNRs are between 47.74 and 54.23 dBs, which are considered good results with regard to the purpose of quality.

VII. CONCLUSIONS

An optimized video steganography approach is designed based on cuckoo search meta-heuristic optimization algorithm. During the execution, coordinates of the optimal cover pixels for embedding are located by cuckoo search population of nests taking into account two considerations: The first one, each secret byte is re-structured into different 5 patterns and be carried by 5 nests to optimize the search process and enhance the security level of information hiding. The second consideration is that based on a lévy flight random walk, the locations of these nests are updated to move from pixel to another in the cover frame's search space. Finally, based on the objective function, the best nest for each inputted secret byte is detected to help in the process of embedding utilizing the 3-3-2 LSB technique.

Experimental results show that the proposed approach is considered a high embedding efficiency approach due to the low modification on the host frames that makes the stego videos have a good quality. PSNR and MSE measurements are used to measure the visual quality and all the obtained experimental results have a PSNR above 47 dBs.

REFERENCES

[1] P. Yadav, N. Mishra, and S. Sharma, "A secure video steganography with encryption based on LSB technique," Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, pp.1-5, 26-28 Dec. 2013.

[2] R. Paul, A.K. Acharya, V.K. Yadav, and S. Batham, "Hiding large amount of data using a new approach of video steganography," in Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), pp.337-343, 26-27 Sept. 2013.

[3] R. Balaji and G. Naveen, "Secure data transmission using video Steganography," in Electro/Information Technology (EIT), 2011 IEEE International Conference on , pp.1-5, 15-17 May 2011

[4] K. Dasgupta, J. K. Mandal, and P. Dutta, "Hash Based Least Significant Bit Technique For Video Steganography(HLSB)", in Proc. of International Journal of Security, Privacy and Trust Management (IJSPTM) , 2012, Vol. 1, No. 2, pp. 1-11.

[5] K. Wang, H. Zhao, and H. Wang, "Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value," Information Forensics and Security, IEEE Transactions on, vol.9, no.5, pp.741-751, May 2014.

[6] AT. Bhole and R. Patel, "Steganography over video file using Random Byte Hiding and LSB technique," Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on , doi: 10.1109/ICCIC.2012.6510230,pp.1–6, 18-20 Dec. 2012.

[7] R.J. Mstafa and K.M. Elleithy, "A highly secure video steganography using Hamming code (7, 4)," in Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island , pp.1-6, 2-2 May 2014 doi: 10.1109/LISAT.2014.6845191

[8] X.S. Yang and S. Deb, "Cuckoo search via lévy flights. In Nature Biologically Inspired Computing,".World Congress on, pages 210–214, 2009.

[9] Y. Kakde, P. Gonnade, and P. Dahiwale, "Audio-video steganography," in Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on , pp.1-6, 19-20 March 2015. doi: 10.1109/ICIIECS.2015.7192885

[10] H.M. Kelash, O.F. Abdel Wahab, O.A. Elshakankiry,and H.S. El-sayed, "Hiding data in video sequences using steganography algorithms," in ICT Convergence (ICTC), 2013 International Conference on , doi: 10.1109/ICTC.2013.6675372, pp.353-358, 14-16 Oct. 2013

[11] K. Dasgupta, J. K. Mondalb, and P. Duttac, " Optimized Video Steganography using Genetic Algorithm (GA)," International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA), 2013 by Elsevier Ltd, Procedia Technology , pp.131 – 137, 2013.

[12] M. E. Eltahir, L. M. Kiah, and B. B. Zaidan, "High Rate Video Streaming Steganography," in Information Management and Engineering, 2009. ICIME '09. International Conference on, 2009, pp. 550-553.

[13] K. Rai, A. Sharma, and M. Tanwar, "Steganography in Compressed Video Stream", Internatonal Journal of Innovative Research in Technology, vol.1, no. 5, pp.824-826, 2014.

[14] M. Pazarci and V. Dipcin, "Data Embedding in Scrambled Digital Video", Proceedings of the 8th IEEE International Symposium on Computers and Communication, 2003, pp. 498-503.

[15] W.M. Aly and A. Sheta," Evaluation of Cuckoo Search Usage for Model Parameters Estimation,". In Max Bramer and Miltos Petridis, editors, Research and Development in Intelligent Systems XXX, pages 443–449. Springer International Publishing, 2013.

[16] W.M. Aly and H.A. Kelleny, "Adaptation of Cuckoo search for Documents Clustering," International Journal of Computer Applications 86(1):4-10, January 2014.

[17] N. Kafri1 and H. Y. Suleiman, "Bit-4 of frequency domain-DCT steganography technique," in Proc. of Networked Digital Technologies, IEEE, 2009, pp. 286-291.